Fiscal Service **Security Rules of Behavior**
January 27, 2025

SUBJECT:
The Bureau of the Fiscal Service (Fiscal Service) Security Rules of Behavior (Rules of Behavior)

PURPOSE:
The Rules of Behavior define responsibilities and procedures for the secure use of Fiscal Service data, equipment, information technology (IT) systems, and facilities. By reading and signing the Rules of Behavior, Users (defined below) acknowledge their responsibility for complying with the Rules of Behavior.

SCOPE:
The Rules of Behavior apply to Users (not public users) who access or maintain any Fiscal Service data, equipment, IT systems, or facilities, regardless of location (e.g., whether you are at your regular duty station or a remote work location). Users are individuals who have access to Fiscal Service data, equipment, IT systems or facilities for the purpose of performing work on behalf of Fiscal Service. Examples of Users include, but are not limited to, Fiscal Service employees and employees of contractors, sub-contractors, and agents. At Fiscal Service's discretion, certain individuals who have access to Fiscal Service data, equipment, IT systems, or facilities may not be considered Users under this definition and as such may not be required to sign these Rules of Behavior. In addition to the rules and requirements contained within this document, Users should note that other federal laws and regulations apply when accessing Fiscal Service resources (e.g., licensing agreements and copyright laws), but are considered outside the scope of this document.

Users SHALL:

Follow these rules regarding Fiscal Service facilities:

- Use facilities properly and follow laws, regulations, and policies governing the use and entrance to such facilities.
- Do not threaten any person or organization.
- Do not commit acts of violence against any person, organization, equipment, or facility.
- Do not bring prohibited items (e.g., weapons) into a Fiscal Service facility.
- Do not use another person's access credential to enter a Fiscal Service facility or secured room.

Follow these rules regarding Fiscal Service data, equipment, and IT systems:

- Use Fiscal Service data, equipment, and IT systems properly and follow laws, regulations, and policies governing the use of such resources (Base Line Security Requirements, (BLSRs), Treasury Information Technology Security Program (TD-P 85-01), the Treasury Security Manual (TD-P 15-71), and Fiscal Service Policies).
- Protect Fiscal Service data, equipment and IT systems from loss, theft, damage, and unauthorized use or disclosure.
- Secure mobile media (paper and digital) based on the sensitivity of the information contained.
- Use appropriate sensitivity markings on mobile media (paper and digital).
- Promptly report any known or suspected security breaches or threats, including lost, stolen, or improper/suspicious use of Fiscal Service data, equipment, IT systems, or facilities to the IT Service Desk at 304-480-7777.
- Do not attempt to circumvent any security or privacy controls.
- Logoff, lock, or secure workstation/laptop to prevent unauthorized access to Fiscal Service IT systems or services.

- Do not read, alter, insert, copy, or delete any Fiscal Service data except in accordance with assigned job responsibilities, guidance, policies, or regulations. The ability to access data does not equate to the authority to access data. In particular, Users must not browse or search Fiscal Service data except in the performance of authorized duties.
- Do not reveal any data processed or stored by Fiscal Service except as required by job responsibilities and within established procedures.
- Do not remotely access Fiscal Service IT systems unless authorized to do so, such as an approved telework agreement authorizing remote access over the bureau's VPN software.
- Do not transport or use Fiscal Service data or equipment outside of the United States or US Territories without written approval from the CSO or CISO.
- Do not connect Fiscal Service equipment to or access a Fiscal Service IT system from a foreign network without written approval from the CSO or CISO.
- Do not install or use unauthorized software or cloud services on Fiscal Service equipment.
- Take reasonable precautions to prevent unauthorized individuals from viewing screen contents or printed documents.
- Do not open e-mail attachments, or click links, from unknown or suspicious sources.
- Be responsible for all activities associated with your assigned user IDs, passwords, access tokens, identification badges, Personal Identity Verification (PIV) cards, or other official identification device or method used to gain access to Fiscal Service data, equipment, IT systems, or facilities.
- Protect passwords and other access credentials from improper disclosure.
- Do not share passwords with anyone else or use another person's password or other access credential such as, but not limited to, someone else's PIV card.
- Use only equipment and software provided by Fiscal Service or that has been approved for use by Fiscal Service's CIO or designee to conduct Fiscal Service business.
- Provide non-work contact information to the bureau to facilitate emergency communications.
- Comply with Fiscal Service social media policy, including restrictions on publishing Fiscal Service information to social media and public websites.

ACCEPTANCE:

I have read the Fiscal Service Security Rules of Behavior and fully understand the security requirements. I further understand that violation of these rules may be grounds for legal and/or administrative action by the Fiscal Service and may result in actions up to and including disciplinary action, termination of access, termination of employment, contract termination, and/or prosecution under federal law.

User's Name: _____ (printed)

User's Signature: _____ (signature)

Date: _____